

Guide for the System Center Monitoring Pack for System Center – Service Manager

Microsoft Corporation

Published: November 22, 2017

Send feedback or suggestions about this document to [mpgfeed@microsoft.com](mailto:mpgfeed@microsoft.com). Please include the name of the monitoring pack guide with your feedback.

The Operations Manager team encourages you to provide feedback on the monitoring pack by providing a review on the monitoring pack’s page in the [Management Pack Catalog](http://go.microsoft.com/fwlink/?LinkID=82105).

Copyright

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.

© 2016 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Windows, and Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

[Guide for the System Center Monitoring Pack for System Center – Service Manager 5](#_Toc402429174)

[Guide History 5](#_Toc402429175)

[Supported Configurations 5](#_Toc402429176)

[Prerequisites 6](#_Toc402429177)

[Mandatory Configuration 6](#_Toc402429178)

[Optional Configuration—Additional Management Packs 6](#_Toc402429179)

[Files in This Monitoring Pack 7](#_Toc402429180)

[Monitoring Pack Purpose 7](#_Toc402429181)

[See Also 8](#_Toc402429182)

[Monitoring Scenarios 8](#_Toc402429183)

[See Also 12](#_Toc402429184)

[How Health Rolls Up 13](#_Toc402429185)

[Services and Workflows Health Monitors 15](#_Toc402429186)

[See Also 16](#_Toc402429187)

[Importing the System Center Monitoring Pack for System Center – Service Manager 16](#_Toc402429188)

[See Also 16](#_Toc402429189)

[Configuring the System Center Monitoring Pack for System Center - Service Manager 17](#_Toc402429190)

[Best Practice: Create a Management Pack for Customizations 17](#_Toc402429191)

[Security Configuration 17](#_Toc402429192)

[Configuring for Agentless Monitoring 19](#_Toc402429193)

[Configuring the Health Rollup Policy 19](#_Toc402429194)

[See Also 20](#_Toc402429195)

[Resources for the System Center Monitoring Pack for System Center – Service Manager 21](#_Toc402429196)

[See Also 21](#_Toc402429197)

[Troubleshooting 22](#_Toc402429198)

[Unable to Detect Failures of the Health Service 22](#_Toc402429199)

[Issue 22](#_Toc402429200)

[Possible Cause 22](#_Toc402429201)

[Resolution 22](#_Toc402429202)

[Discovery Fails to Run 22](#_Toc402429203)

[Issue 22](#_Toc402429204)

[Possible Cause 22](#_Toc402429205)

[Resolution 22](#_Toc402429206)

[See Also 23](#_Toc402429207)

[Appendix A: Monitoring Pack Discovery 23](#_Toc402429208)

[Service Manager Management Server Discovery 23](#_Toc402429209)

[Data Warehouse Management Server Discovery 24](#_Toc402429210)

[Service Manager Properties Discovery 25](#_Toc402429211)

[Data Warehouse Management Server Properties Discovery 26](#_Toc402429212)

[Service Manager Management Group and Data Warehouse Management Group Discovery 27](#_Toc402429213)

[Service Manager Data Warehouse Database Discovery 28](#_Toc402429214)

[See Also 29](#_Toc402429215)

[Appendix B: Monitoring Pack Scripts 29](#_Toc402429216)

[See Also 30](#_Toc402429217)

# Guide for the System Center Monitoring Pack for System Center – Service Manager

The System Center Monitoring Pack for System Center – Service Manager helps you manage your Service Manager infrastructure by monitoring the health of the Service Manager management servers and services. You can use this monitoring pack to monitor the management servers, data warehouse management servers, workflows, and services in **System Center 2012** – Service Manager, **System Center 2012 SP1**- Service Manager, **System Center 2012 R2**- Service Manager, and **System Center 2016**- Service Manager.

For Service Manager to function correctly, the management servers and the services must function correctly. The monitoring pack for System Center - Service Manager alerts you about problems with these management servers and services so that you can troubleshoot and repair any problems that may occur.

This guide is based on version 7.5.7487.0 of the System Center Monitoring Pack for **System Center 2012** – Service Manager, **System Center 2012 SP1**- Service Manager, **System Center 2012 R2**- Service Manager, and **System Center 2016**- Service Manager.

### Guide History

|  |  |
| --- | --- |
| Release Date | Changes |
| May 2012 | Original release of this guide. |
| January 2015 | Updated Version to 7.5.3079.183 |
| January 2015 | Updated platform support to include System Center 2012 SP1- Service Manager and System Center 2012 R2- Service Manager. |
| October 2016 | Updated platform support to include System Center 2016- Service Manager. |
| November 2017 | TLS 1.2 support added for System Center 2016- Service Manager and System Center 2012 R2- Service Manager |

### Supported Configurations

To monitor parts in System Center Service Manager, use this monitoring pack with System Center Operations Manager. This monitoring pack requires agentless monitoring (monitoring of computers without agents) and a dedicated Operations Manager management group.

The monitoring pack for System Center Service Manager version 7.5.7487.0 supports all the configurations that are supported by **System Center 2012** – Service Manager, **System Center 2012 SP1**- Service Manager, **System Center 2012 R2**- Service Manager, and **System Center 2016**- Service Manager.

Service Manager supports Microsoft SQL Server clustering for the databases and Network Load Balancing (NLB) for the Service Manager management servers and portals. In these topologies, the individual parts are monitored individually, regardless of the existence of NLB.

The following table provides details about the supported configurations for the monitoring pack for Service Manager.

|  |  |
| --- | --- |
| Configuration | Support |
| Service Manager management servers | Yes, all supported configurations and all supported deployment topologies |
| Servers on which workflows run | Yes |
| Data warehouse management servers | Yes |
| Clustered servers | Yes |
| Agentless monitoring | Yes |
| Virtual environment | Yes |

### Mandatory Configuration

Before you import the monitoring pack for System Center - Service Manager, you must update the Service Manager Database Account Run As profile that is provided in this monitoring pack. For information about this update, see the “Security Configuration” section in [Configuring the System Center Monitoring Pack for System Center - Service Manager](#z1ad1234d1d604c988fe8001d6c4c1f93).

You should also ensure that the Service Manager management servers are configured for agentless monitoring. For information about how to configure agentless monitoring, see [Agentless Monitoring in Operations Manager](http://go.microsoft.com/fwlink/p/?LinkId=245180). Be sure to read the “Security Configuration” section in [Configuring the System Center Monitoring Pack for System Center - Service Manager](#z1ad1234d1d604c988fe8001d6c4c1f93) after you follow the instructions in the link.

### Optional Configuration—Additional Management Packs

Because the monitoring pack for System Center - Service Manager has no dependencies on other management packs, you can use it independently. However, Service Manager relies on other applications, such as SQL Server, to run correctly. It is assumed that all applications that Service Manager relies on are also monitored continually by their respective management packs. By having these additional management packs available, the number of Service Manager parts that the monitoring pack for System Center - Service Manager must monitor is reduced. For example, the SQL Server management pack monitors the Service Manager database, and the Internet Information Services (IIS) Management Pack monitors the Self Service Portal web pages. The monitoring pack for System Center - Service Manager does not monitor these Service Manager parts.

Still, the monitoring pack for System Center - Service Manager does monitor the interaction between Service Manager and various parts in other products. For example, the monitoring pack for System Center - Service Manager monitors the System Center Data Access Service and the System Center Management Configuration service connectivity to the Service Manager database.

For comprehensive monitoring of Service Manager, we recommend deploying the following management packs:

 Windows Server Management Pack for monitoring the operating system of all Service Manager management servers.

 SQL Server Management Pack for monitoring the server that is running SQL Server and that is hosting the Service Manager database, the DWStagingAndConfig database, and the DWRepository and DWDatamart databases. The SQL Server Management Pack is also used for monitoring the server that hosts SSRS, which Service Manager uses for generating reports.

 Internet Information Services (IIS) Management Pack for monitoring IIS on the computers that are running the Service Manager Self Service portals.

 ASP.Net Management Pack. This management pack is used for monitoring Microsoft ASP.Net on the server that is running the Service Manager Self Service portals.

### Files in This Monitoring Pack

The monitoring pack for System Center - Service Manager includes the following files:

 Microsoft System Center Management Pack for Service Manager.msi:

 Microsoft.SystemCenter.ServiceManager.Discovery

 Microsoft.SystemCenter.ServiceManager.Library

 Microsoft.SystemCenter.ServiceManager.Monitoring

 EULA.rtf

 Nineteen language pack files that support the following ten languages: English, Chinese Simplified, Chinese Traditional, French, German, Italian, Japanese, Korean, Portuguese (Brazil), Portuguese (Portugal), Russian, Spanish, Dutch, Polish, Hungarian, Sami, Southern (Sweden), Czech, and Turkish.

# Monitoring Pack Purpose

The purpose of using the System Center Monitoring Pack for System Center - Service Manager is to help centralize the overall monitoring in your organization to one location, the Operations Manager console. The monitoring pack also provides instructions to end users about how to repair problems that may be detected during monitoring. This helps to simplify maintenance and reduce the number of support calls to Microsoft.

In this section:

 [Monitoring Scenarios](#z9f62c8a83e6f4edcbdc2b73699f387d0)

 [How Health Rolls Up](#z91ff9e64670a45a09a85e0c70126b99d)

For details about the discoveries, rules, monitors, views, and reports that this monitoring pack contains, see [Appendix A: Monitoring Pack Discovery](#z975f0805fab94adaab0d9e70f80afaf8).

## See Also

[Guide for the System Center Monitoring Pack for System Center – Service Manager](#zbb1b80b3a4f4465797ceeb2e6cd6544d)

# Monitoring Scenarios

The following table describes the monitoring scenarios that are included in this System Center Monitoring Pack for System Center – Service Manager.

|  |  |  |
| --- | --- | --- |
| Monitoring scenario | Description | Associated rules and monitors |
| Services Running on the Management Server | Monitoring the following services:  **** System Center Data Access Service  **** System Center Management Configuration service  **** System Center Management service | **** Microsoft.ServiceManager.SDKService.ServiceMonitor  Indicates whether the System Center Data Access Service is running.  **** Microsoft.ServiceManager.ConfigurationService.ServiceMonitor  Indicates whether the System Center Management Configuration service is running.  **** Microsoft.ServiceManager.HealthService.AvailabilityHealthRollup  Indicates whether the System Center Monitoring Pack for System Center – Service Manager service is running and whether it is available. |
| Workflows Running on a Service Manager Management Server | Monitoring the following workflows:  **** Windows Workflow Foundation (WWF) workflows  **** System Workflows  **** Connectors |  |
| Windows Workflow Foundation Workflows | Monitoring rules check the value in the workflow Status column. Depending on the value, they detect the following possible workflow failures:  **** A workflow cannot be triggered, or the associated tasks cannot be submitted.  **** A workflow finishes running successfully, but the output has an exception.  **** A workflow starts running but times out. This indicates that the workflow ran for more than 25 minutes.  **** A workflow fails while running. | The following rules are used for this monitoring task, and the default interval for these rules is four hours:  **** Microsoft.SystemCenter.ServiceManager.WWF.Monitoring.RuleException:  Status of 2 indicates that the workflow ran successfully, but it has an exception in the output.  **** Microsoft.SystemCenter.ServiceManager.WWF.Monitoring.RuleRunning:  Status of 1 or 2 indicates that the workflow has been running for more than 25 minutes, and it is likely that the workflow timed out.  **** Microsoft.SystemCenter.ServiceManager.WWF.Monitoring.RuleFailed:  Status of 3 indicates that the workflow failed.  **** Microsoft.SystemCenter.ServiceManager.WWF.Monitoring.RuleTaskSubmitError:  Status of NULL indicates that the workflow cannot submit tasks, possibly as a result of an infrastructure error. In this case, there is no entry in the JobStatus table, and Status is set to NULL.  A single monitor displays the overall health of the WWF workflows. This monitor uses an Object Linking and Embedding Database (OLEDB) probe, and it returns a count of the number of rows with any one of the failure conditions. If the count is 0, indicating that there are no failures, the monitor is green. If the count is not 0, the monitor is yellow, and it generates an alert message that directs the user to look for details in the active alerts view. |
| Linking Framework Workflows | Monitoring rules check the value in the connector Status column. Depending on the value, they detect the following possible workflow failures:  **** The connector was created, but data synchronization did not start after more than 5 minutes.  **** Data synchronization starts and completes but with an error.  **** The connector is in an unknown status. | The following rules are used for this monitoring task, and the default interval for these rules is four hours:  **** Microsoft.SystemCenter.ServiceManager.Lfx.Monitoring.NeverRun:  Status of NeverRun, combined with a difference between timestarted and timefinished that is greater than 5 minutes, causes the generation of an alert.  **** Microsoft.SystemCenter.ServiceManager.Lfx.Monitoring.FinishedwithError:  Status of FinshedwithError indicates that an error occurred during data synchronization.  **** Microsoft.SystemCenter.ServiceManager.Lfx.Monitoring.Unknown:  Status that is unknown causes the generation of an alert.  A monitor checks for any of the failures. If there is a record that indicates a NeverRun, FinishedWithError, or Unknown status, an alert is generated. |
| Grooming Workflows | Monitoring for the following possible failures:  **** A workflow fails with a status of 2.  **** A workflow times out. | A monitor extracts the status for the grooming workflows from the InternalJobHistory table. When the monitor detects a failure, it generates an alert with a generic message that references grooming workflows. In this case, the state of the monitor is set to red.  If a workflow’s status is Started and it has been running for more than 25 minutes, it is likely that the workflow timed out. However, in the case of the SubscriptionGroomingLogs workflow, the interval is set to 15 minutes because the run time for that workflow is less than 15 minutes. |
| Operations Manager Connector Workflows | Monitoring for failures that are associated with data synchronization and other failures that are detected in event logs. | A monitor that checks event logs to detect problems and failures. The following events cause the generation of an alert, and they change the state of the monitor to red:  **** Event ID 34073 – Unexpected error while creating/updating incident from alert.  **** Event ID 34076 – Underlying Linking Framework connector instance for sync workflow is missing.  **** Event ID 34080 – Generic error from the Service Manager SDK.  **** Event ID 34081 – Unhandled exception during synchronization.  **** Event ID 34090 - Scheduled synchronization cannot start.  For the monitor to turn back to a green/healthy state, the following events must be detected:  **** Event ID 34084 - CI synchronization.  **** Event ID 34089 – Processed alert in Service Manager via connector. |

## See Also

[Monitoring Pack Purpose](#z000e14b01e084425ac93784f1c8cad1e)

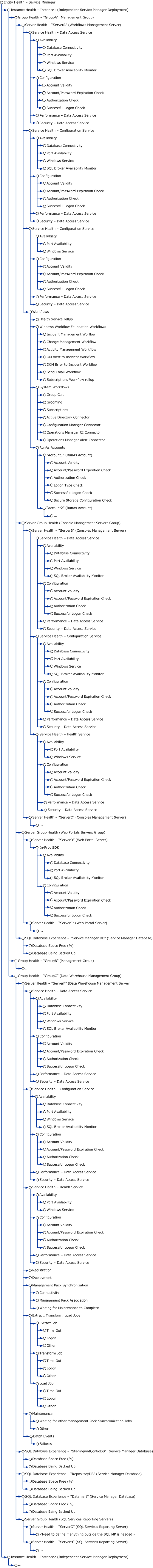
# How Health Rolls Up

The System Center Monitoring Pack for System Center – Service Manager monitors the health of services and workflows to determine the health of Service Manager management servers. The health of the management servers is then determined based on the aggregated health of these services and workflows. For Service Manager data warehouse management servers, the same process is used. However, workflows are not monitored; therefore, the health of the data warehouse management servers is determined based on the aggregated health of services only.

Health rolls up from the management-servers level to the management-groups level and then from the management-groups level to the application level. The application, at the top level of the health diagram, displays the overall health of Service Manager.

By default, health rollup from level to level is configured by using the Percentage Policy, and the percentage is set to 50. For example, this means that at least 50 percent of the management servers that are being monitored must be healthy for the respective management group to be healthy.

The following diagram shows how the health states of objects roll up in this monitoring pack. It displays the health rollup of the System Center Data Access Service, the Health service, and the System Center Management Configuration service. In addition, it displays the health rollup of workflows. The Workflows health rollup displays the actual health status of the workflows.



## Services and Workflows Health Monitors

The following are all the monitors in this monitoring pack. These basic monitors monitor for availability. Security, performance, and configuration are not monitored in this release.

 System Center Data Access Service availability. The System Center Data Access Service is a Windows service that is used for communication between the Service Manager management servers and the Service Manager databases and for importing management packs.

The following monitors are used to monitor the availability of the System Center Data Access Service:

 AzMan—database connectivity

 Data Access service—database connectivity

 Data Access service—port availability

 Data Access service—Windows service

 SQL Server Broker Availability Monitor

 Health service availability. The Health service is a Windows service that is used for running workflows under the appropriate identity and for the appropriate lifetime. The Health service is the Operations Manager agent. It cannot monitor itself if it is not available.

The following monitors are used to monitor the availability of the Heath service:

 RunAs accounts:

 Action Account Type Check

 RunAs Account Monitoring Check

 RunAs Account/Password Expiration Check

 RunAs Authorization Check

 RunAs Logon Type Check

 RunAs Successful Logon Check

 Secure Storage Configuration Check

 System Center Management Configuration service availability. The System Center Management Configuration service is a Windows service that provides specific Health service configurations to all Health services in the management group.

The following monitors are used to monitor the availability, and to detect the following failure conditions of the System Center Management Configuration service:

 Management Configuration service database connectivity:

 Management Configuration service could not connect to the database in the last 30 minutes (Critical level)

 Management Configuration service could not connect to the database in the last 15 minutes (Warning level)

 Management Configuration service—Windows service state

 Workflow availability. Service Manager uses workflows to automate information technology (IT) processes and reduce the amount of work that IT analysts must perform manually.

The following monitors are used to monitor the availability of workflows:

 Grooming Workflows

 Linking Frameworks Workflows

 Operations Manager Connector Workflows

 Windows Workflow Foundation (WWF) Workflows

## See Also

[Monitoring Pack Purpose](#z000e14b01e084425ac93784f1c8cad1e)

# Importing the System Center Monitoring Pack for System Center – Service Manager

To ensure that you do not receive alerts in the Operations Manager console that relate to failed Object Linking and Embedding Database (OLEDB) modules and synthetic transaction failures, we recommend that you perform the monitoring pack import tasks in the following order:

1. Import the Library (Microsoft.SystemCenter.ServiceManager.Library) monitoring pack separately.

2. Populate the Service Manager Run As profile.

3. Import the Discovery (Microsoft.SystemCenter.ServiceManager.Discovery) monitoring pack.

4. Wait until discovery is complete and until properties of all objects are fully discovered. The default intervals for discovery are every 24 hours, with varying running times during the day. You can use overrides to change these default values.

5. Import the Monitoring (Microsoft.SystemCenter.ServiceManager.Monitoring) monitoring pack.

## See Also

[Guide for the System Center Monitoring Pack for System Center – Service Manager](#zbb1b80b3a4f4465797ceeb2e6cd6544d)

# Configuring the System Center Monitoring Pack for System Center - Service Manager

This topic contains guidance for configuring and tuning the System Center Monitoring Pack for System Center – Service Manager:

 [Best Practice: Create a Management Pack for Customizations](#z2)

 [Security Configuration](#z3)

 [Security Configuration](#z3)

 [Security Configuration](#z3)

## Best Practice: Create a Management Pack for Customizations

By default, Operations Manager saves all customizations, such as overrides to the Default Management Pack. As a best practice, you should instead create a separate management pack for each sealed management pack that you want to customize.

When you create a management pack for the purpose of storing customized settings for a sealed management pack, it is helpful to base the name of the new management pack on the name of the management pack that it is customizing, for example, “Customizations to the Service Manager Monitoring Pack.”

Creating a new management pack for storing customizations of each sealed management pack makes it easier to export the customizations from a test environment to a production environment. It also makes it easier to delete a management pack, because you must delete any dependencies before you can delete a management pack. If customizations for all management packs are saved in the Default Management Pack and you want to delete a single management pack, you must first delete the Default Management Pack, which also deletes customizations to other management packs.

## Security Configuration

The System Center Monitoring Pack for System Center – Service Manager introduces a new Run As profile, named the Service Manager Database Account profile, which is used to access the Service Manager databases and the staging and configuration DWStagingAndConfig databases.

Before you import the management pack, you must add a Run As account to the Service Manager Database Account profile, and then add the Run As account to the Service Manager database server and to the server that hosts the staging and configuration database, DWStagingAndConfig, as described in the following sections. The Run As account that is associated with the Service Manager Database Account profile is then used to access the Service Manager database and the DWStagingAndConfig database.

Perform the following procedure in the Operations Manager console. For more information about the detailed steps of these procedures, see [Managing Run As Accounts and Profiles](http://go.microsoft.com/fwlink/p/?LinkId=245183) on Microsoft TechNet.

To add a Run As account to the Service Manager Database Account profile

|  |
| --- |
| 1. Open the Operations Manager console.  2. Create a new Run As account in the Create Run As Account Wizard. On the General Properties page, in the Run As Account type box, click Windows.  Notes  The Run As account that you create must be configured to have logon permissions to the Service Manager management server and to the Service Manager data warehouse management server that are being monitored by the Operations Manager agent. Also, the account must have permissions to access the following registry keys, both on the Service Manager management server and on the Service Manager data warehouse management server:   HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\System Center   HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\ServerManagement Groups  3. Locate and then right-click the Service Manager Database Account profile, to start the Run As Profile Wizard. On the Run As Accounts page, add the new Run As account. |

Perform the following procedure on the Service Manager database server and on the server that hosts the staging and configuration DWStagingAndConfig database.

To update the Service Manager database servers by using the new Service Manager Database Account profile

|  |
| --- |
| 1. On the server that hosts the Service Manager database and on the server that hosts the staging and the configuration database, click Start, point to Programs, point to Microsoft SQL Server <version>, and then click SQL Server Management Studio.  2. In the Connect to Server dialog box, in the Server Name list select the server and instance for your SQL Server that contains the Service Manager database, and then click Connect.  3. In the Object Explorer pane, expand Security, right-click Logins, and then click New Login.  4. In the Login – New dialog box, type a logon name in Login name, or use Search to locate an account.  5. Click OK.  6. In the Object Explorer pane, expand Databases, <Service Manager database name>, and Security. Right-click Users, and then click New User.  7. In the Database User – New dialog box, in the User name box, type a user name.  8. Click the Login name ellipsis (…) button to locate the logon that you just created, and then click OK.  9. In the Object Explorer pane, browse to Databases, <Service Manager database name>, Security, Roles, and then expand Database Roles.  10. Right-click db\_datareader, and then click Properties.  11. In the Properties dialog box, click Add.  12. In the Select Database User or Role box, click Browse, and in the Browse for Objects dialog box, select the user that you created previously.  13. Click OK to close all the dialog boxes. |

## Configuring for Agentless Monitoring

To enable monitoring of System Center – Service Manager using System Center – Operations Manager, this monitoring pack relies on agentless monitoring of Service Manager systems.

The following configurations are required to ensure that agentless monitoring is possible:

 Any firewall and routing are configured to support monitoring of the Service Manager management server from the designated proxy system. Access to the Service Manager and data warehouse databases must be possible because it is required by the proxy agent in one of the monitoring scenarios.

 The Windows Management Instrumentation (WMI) service is running on the proxy agent and on all Service Manager management servers that you want to monitor.

 The proxy system is able to establish a remote WMI connection to all Service Manager management servers. By default, this is possible if the service account that is used for proxy monitoring has administrative privileges on the Service Manager management servers.

 The account that is used for the Database Run As Profile also has these same privileges; therefore, it can access registry keys remotely from the proxy agents.

In low-privilege environments, it might not be desirable to grant these accounts full administrative access on Service Manager systems. For these environments, follow the instructions in [Authorize WMI users and set permissions](http://technet.microsoft.com/en-us/library/cc771551.aspx) to allow the accounts the following permissions on the WMI Default namespace:

 Enable Account

 Remote Enable

 Execute Methods

For more information about managing WMI security, see [Managing WMI Security](http://technet.microsoft.com/en-us/library/cc731011.aspx).

## Configuring the Health Rollup Policy

By default, the Health Rollup Policy in the System Center Monitoring Pack for System Center – Service Manager is configured to use the Percentage Policy, with the percentage set to 50. Typically, this setting works well for deployments that consist of one or two management servers in the management group.

However, this default configuration might not be optimal in some environments. Depending on the specific Service Manager deployment in your organization, you might want to modify this default setting. You can change the percentage number based on requirements and thresholds that are acceptable in your organization.

You can use the following procedure to change the percentage number for the SCSM Management Group class, the DW Management Group class, or the Service Manager class.

To change the percentage of the Health Rollup Policy

|  |
| --- |
| 1. Log on to the computer that has an account that is a member of the Operations Manager Administrators user role or the Operations Manager Authors user role for the Operations Manager management group.  2. In the Operations console, click the Authoring button.  3. In the Authoring pane, expand Authoring, expand Management Pack Objects, and then click Monitors.  4. In the Monitors pane, click Change Scope.  5. In the Scope Management Pack Objects dialog box, click View all targets, and ensure that nothing is selected in the list.  6. Select SCSM Management Group from the list, and then click OK. You can select DW Management Group or Service Manager if you want to change the percentage for these classes.  7. In the Monitors pane, expand SCSM Management Group, expand Entity Health, and then expand Availability.  8. Right-click SCSM Management Group Availability, click Overrides, click Override the Monitor, and then click For all objects of class: SCSM Management Group.  9. In the Override Properties dialog box, click Show Monitor Properties.  10. In the SCSM Management Group Availability Properties dialog box, click the Health Rollup Policy tab. Change the percentage under the option Worst state of the specified percentage of members in good health state (the option itself is dimmed).  11. Close all the dialog boxes to save the change. |

## See Also

[Guide for the System Center Monitoring Pack for System Center – Service Manager](#zbb1b80b3a4f4465797ceeb2e6cd6544d)

# Resources for the System Center Monitoring Pack for System Center – Service Manager

The following links contain information about common tasks that are associated with System Center Monitoring Packs:

 [Administering the Management Pack Life Cycle](http://go.microsoft.com/fwlink/?LinkId=211463)

 [How to Import an Operations Manager Management Pack](https://technet.microsoft.com/en-us/library/hh212691(v=sc.12).aspx)

 [How to Monitor Using Overrides](http://go.microsoft.com/fwlink/?LinkID=117777)

 [How to Create a Run As Account in Operations Manager](https://technet.microsoft.com/en-us/library/hh321655(v=sc.12).aspx)

 [How to Modify an Existing Run As Profile](http://go.microsoft.com/fwlink/?LinkID=165412)

 [How to Export Management Pack Customizations](http://go.microsoft.com/fwlink/?LinkId=209940)

 [How to Remove a Management Pack](http://go.microsoft.com/fwlink/?LinkId=209941)

For questions about Operations Manager and monitoring packs, see the [System Center Operations Manager community forum](http://go.microsoft.com/fwlink/?LinkID=179635).

A useful resource is the [System Center Operations Manager Unleashed blog](http://opsmgrunleashed.wordpress.com/), which contains “By Example” posts for specific monitoring packs.

For additional information about Operations Manager, see the following blogs:

 [Operations Manager Team Blog](http://blogs.technet.com/momteam/default.aspx)

 [Kevin Holman's OpsMgr Blog](http://blogs.technet.com/kevinholman/default.aspx)

 [Thoughts on OpsMgr](http://thoughtsonopsmgr.blogspot.com/)

 [Raphael Burri’s blog](http://rburri.wordpress.com/)

 [BWren's Management Space](http://blogs.technet.com/brianwren/default.aspx)

 [The System Center Operations Manager Support Team Blog](http://blogs.technet.com/operationsmgr/)

 [Ops Mgr ++](http://blogs.msdn.com/boris_yanushpolsky/default.aspx)

 [Notes on System Center Operations Manager](http://blogs.msdn.com/mariussutara/default.aspx)

Important

All information and content on non-Microsoft sites is provided by the owner or the users of the website. Microsoft makes no warranties, express, implied, or statutory, as to the information at this website.

## See Also

[Guide for the System Center Monitoring Pack for System Center – Service Manager](#zbb1b80b3a4f4465797ceeb2e6cd6544d)

# Troubleshooting

Use the following tips for troubleshooting issues with the System Center Monitoring Pack for System Center – Service Manager.

## Unable to Detect Failures of the Health Service

### Issue

Problems with the Service Manager Health service are detected as issues with the Operations Manager Health service.

### Possible Cause

If both Service Manager and an Operations Manager agent are running on the same server, they are sharing the Health service. Therefore, if the Health service is experiencing issues, these issues might affect both applications.

### Resolution

None. However, when you are investigating issues with the Operations Manager agent on servers where Service Manager is also present, remember that the issues might be caused by Service Manager.

## Discovery Fails to Run

### Issue

The Diagram view is not displaying any discovered objects, but the Windows Computers view displays a Service Manager instance. In addition, there might be an alert indicating that Agent proxy is not enabled.

### Possible Cause

This is probably because the Agent proxy is not enabled.

### Resolution

Enable the Agent proxy if it is disabled.

If discovery does not run, check the event log on the Service Manager management server. It might contain an error message where Source is Health Service Modules, EventID is 11852, and the Details string is as follows:

“OleDb Module encountered a failure 0x80004005 during execution and will post it as output data item. Unspecified error: [DBNETLIB][ConnectionOpen (Connect()).]SQL Server does not exist or access denied”

This typically indicates that the Run As account for the Service Manager monitoring pack is misconfigured or has insufficient privileges to access the database. Ensure that the Run As account has read access to the database. For information about adding a Run As account to the Service Manager Database Account profile, see Security Considerations.

Otherwise, if discovery does not seem to be running on its scheduled time, you can perform the following steps:

1. Clear the Health service monitoring pack cache on the Service Manager management server.

2. After you clear the cache, remove the System Center Monitoring Pack for System Center – Service Manager from Operations Manager, and then import it again.

3. Override the discovery time.

## See Also

[Guide for the System Center Monitoring Pack for System Center – Service Manager](#zbb1b80b3a4f4465797ceeb2e6cd6544d)

# Appendix A: Monitoring Pack Discovery

The System Center Monitoring Pack for System Center – Service Manager discovers the object types that are described in the following sections. Objects are discovered in several steps. The initial discovery discovers instances of Service Manager management servers and data warehouse management servers. Subsequent discoveries populate these instances with further details about the instances. Not all of the objects are automatically discovered. Use overrides to discover those objects that are not discovered automatically.

Discovery runs one time on import of this management pack, and then it runs on a recurring schedule. The default intervals for discovery are every 24 hours, with varying running times during the day. You can use overrides to change these default values.

## Service Manager Management Server Discovery

This discovery applies to all server computers. It performs a registry check on each targeted server to determine whether the server computer is a Service Manager management server.

This discovery checks the following registry keys:

 SOFTWARE\Microsoft\System Center\2010\Service Manager\Setup

 SOFTWARE\Microsoft\System Center\2010\Common\SDK Service\SDK Service Type

 SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Server Management Groups

If the first and the last registry keys exist on the server and the value of the second registry key equals 1, that server is determined to be a Service Manager management server. In this case, the discovery data that is returned for that server is the PrincipalName and DisplayName property set.

Discovery Information

|  |  |  |
| --- | --- | --- |
| Interval | Enabled | When to Enable |
| Every 24 hours. | True | Not applicable. |

Related Rules

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Rule | Data Source | Alert | Notes | Corresponding Monitor | Enabled | When to Enable |
| Microsoft.SystemCenter.ServiceManager.SmManagementServer.Discovery | Script - SmManagementServerDiscovery.vbs | N/A | Alert generated after 3 repeated alerts within 5 minutes | N/A | True | N/A |

## Data Warehouse Management Server Discovery

This discovery applies to all server computers. It performs a registry check on each targeted server to determine whether the server computer is a data warehouse management server.

This discovery checks the following registry keys:

 SOFTWARE\Microsoft\System Center\2010\Service Manager\Setup

 SOFTWARE\Microsoft\System Center\2010\Common\SDK Service\SDK Service Type

 SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Server Management Groups

If the first and the last registry keys exist on the server and the value of the second registry key equals 2, that server is determined to be a data warehouse management server. In this case, the discovery data that is returned for that server is the PrincipalName and DisplayName property set.

Discovery Information

|  |  |  |
| --- | --- | --- |
| Interval | Enabled | When to Enable |
| Every 24 hours. | True | Not applicable |

Related Rules

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Rule | Data Source | Alert | Notes | Corresponding Monitor | Enabled | When to Enable |
| Microsoft.SystemCenter.ServiceManager.DwManagementServer.Discovery | Script - DWManagementServerDiscovery.vbs | N/A | Alert generated after 3 repeated alerts within 5 minutes | N/A | True | N/A |

## Service Manager Properties Discovery

This discovery runs after a successful discovery of Service Manager. It discovers properties of Service Manager, such as the management group name and the Service Manager database name.

Discovery Information

|  |  |  |
| --- | --- | --- |
| Interval | Enabled | When to Enable |
| Every 24 hours, at 01:00 | True | Not applicable |

Related Rules

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Rule | Data Source | Alert | Notes | Corresponding Monitor | Enabled | When to Enable |
| Microsoft.SystemCenter.ServiceManager.SmManagementServerProperties.Discovery | Script - ManagementServerPropertyDiscovery.vbs | N/A | Alert generated after 3 repeated alerts within 5 minutes | N/A | True | N/A |

## Data Warehouse Management Server Properties Discovery

This discovery runs after a successful discovery of the data warehouse. This discovery runs a Visual Basic Scripting Edition (VBScript) that populates properties of the data warehouse server instance. Properties such as ManagementGroupName, DataMartDbName, and StagingDbName are populated by reading registry key values. This discovery also runs a SQL Server query to identify the Service Manager management groups that the current server’s management group is connected to.

Discovery Information

|  |  |  |
| --- | --- | --- |
| Interval | Enabled | When to Enable |
| Every 24 hours, at 01:00 | True | Not applicable |

Related Rules

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Rule | Data Source | Alert | Notes | Corresponding Monitor | Enabled | When to Enable |
| Microsoft.SystemCenter.ServiceManager.DwManagementServerProperties.Discovery | Script - DwMgtServerPropDiscovery.vbs | N/A | Alert generated after 3 repeated alerts within 5 minutes | N/A | True | N/A |

## Service Manager Management Group and Data Warehouse Management Group Discovery

These are the final discoveries that populate the properties of Service Manager management groups and data warehouse management groups. These discoveries are based on the instances of the respective management servers that were found in the Operations Manager instance space.

These discoveries connect to the Operations Manager database, and they run queries to determine whether instances of the Service Manager management server or the data warehouse management server exist. Properties of the instances that were found are then returned.

Discovery Information

|  |  |  |
| --- | --- | --- |
| Interval | Enabled | When to Enable |
| Every 24 hours, at 14:00 | True | Not applicable |

Related Rules

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Rule | Data Source | Alert | Notes | Corresponding Monitor | Enabled | When to Enable |
| Microsoft.SystemCenter.ServiceManager.SmManagementGroup.Discovery | Script - SmManagementGroupDiscovery.vbs | N/A | Alert generated after 3 repeated alerts within 5 minutes | N/A | True | N/A |
| Microsoft.SystemCenter.ServiceManager.DwManagementGroup.Discovery | Script - DwManagementGroupDiscovery.vbs | N/A |  | N/A | True | N/A |

## Service Manager Data Warehouse Database Discovery

This discovery searches all data warehouse servers, searching for the data warehouse staging database.

Discovery Information

|  |  |  |
| --- | --- | --- |
| Interval | Enabled | When to Enable |
| Every 24 hours, at 01:00 | True | Not applicable |

Related Rules

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Rule | Data Source | Alert | Notes | Corresponding Monitor | Enabled | When to Enable |
| Microsoft.SystemCenter.ServiceManager.Dw2012Database. | Script - Dw2012DatabaseDiscovery.VBS | N/A |  | N/A | True | N/A |

## See Also

[Guide for the System Center Monitoring Pack for System Center – Service Manager](#zbb1b80b3a4f4465797ceeb2e6cd6544d)

# Appendix B: Monitoring Pack Scripts

The following scripts are included in the System Center Monitoring Pack for System Center – Service Manager. They are used for discovery.

|  |  |
| --- | --- |
| Script | Purpose |
| ManagementServerDiscovery.js | Populates the properties of the Service Manager management server. Applies to the Service Manager management server. |
| DwMgtServerPropDiscovery.vbs | Populates properties of the data warehouse management server. Applies to the data warehouse management server. |
| DwManagementGroupDiscovery.vbs | Creates an instance of a data warehouse management group and the Service Manager application. Applies to the data warehouse management server. |
| SmManagementGroupDiscovery.js | Creates an instance of the Service Manager management group. Applies to the Service Manager management server. |
| Dw2012DatabaseDiscovery.VBS | Discovers the data warehouse staging database. |

## See Also

[Guide for the System Center Monitoring Pack for System Center – Service Manager](#zbb1b80b3a4f4465797ceeb2e6cd6544d)